Security Operations Effectiveness

Security professionals' overconfidence in security tools leads to data breaches, vulnerabilities and wasted time and money

Overview

Today's security operations teams face an unrelenting stream of attacks from both outside and inside of their organizations. Security operations teams are dealing with tool sprawl which may inadvertently compromise their security tools' capabilities, while misconfigurations can result in attacks through capable devices. A security professional can implement temporary rules to authorize short-term contractor access no longer needed or accidentally turn off a setting that may not get noticed.

This report investigates the current thinking of security operations teams and senior management to understand how they validate that their security solutions are working and if they are defending their organizations as expected. In addition, the research sought to understand the value and concerns of running security assessments against production systems.

Overconfidence relating to actual security operations has led two-thirds of companies to operate overlapping solutions (half by accident), resulting in wasted budget with no improvement in security posture.

KEYSIGHT TECHNOLOGIES

Executive Summary

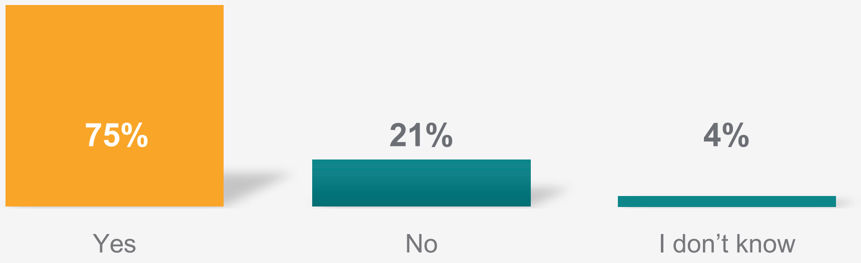
This report reveals that security experts are overconfident that their security solutions are working as intended and breaches continue to happen. The research finds 75 percent of companies surveyed have been breached on average once each year. Research indicates that barely half of security professionals are confident in their current security solutions.

Security professionals admit that they test infrequently. Only one-third of companies surveyed have tested their security solutions in the last 30 days. Just over 20 percent of companies utilize internal and external security testing. Only half of security teams practice breach response and remediation. Further, just 35 percent of those surveyed test and validate their security defense operations. This lack of knowledge of actual security solution operations has led two-thirds of companies to invest in and operate overlapping solutions (half by accident), resulting in wasted budget with no improvement in security posture.

A strong majority of security professionals surveyed, 86 percent of respondents, recognize value in security test solutions that can actively test their company's security products and posture, using both internal and external attack vectors.

75% of Companies Succumbed to Security Breaches

Has your business ever experienced a cyber security breach (intrusion, virus, bot, hack, etc.)?



The Results

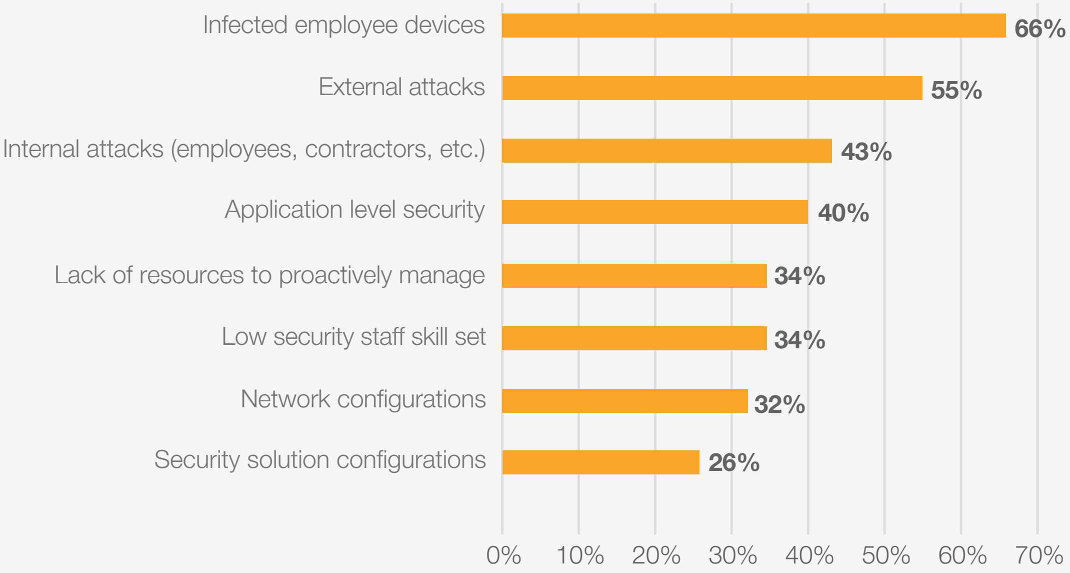
Security Professionals Worry about Defending their Organizations on Multiple Fronts

Security professionals are worried about the next cybersecurity attack and their abilities to defend their organizations.

Those surveyed indicate that they are concerned about security against an ever-increasing attack surface; they worry about insider threats with 66 percent worried about infected employee devices; while 34 percent worried about a low security staff skill set. Fifty-five percent of those surveyed also worry about the risk of external attacks.

Professionals Worry about Defending Numerous Attack Fronts

In your experience, which of the following pose the greatest security risks?



Security professionals are confident in their security tools and their tools' capabilities, but they have underlying concerns.

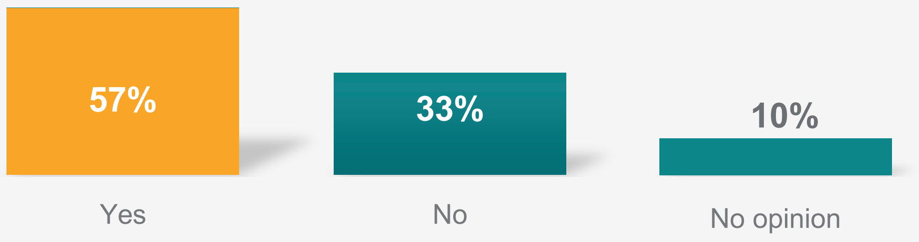
The survey indicates that 57 percent are confident in their security solutions' capabilities. But those surveyed indicated that configurations were a concern: network configurations (32 percent); security solution configurations (26 percent); and application level security (40 percent).

When asked if their security team realized that a security solution was not working as expected, 50 percent of those surveyed answered yes, but they realized it only after a breach.

These figures reveal that security professionals are overconfident in their security infrastructure. While they believe that their security tools are working, the operational reality is very different. Cyberattacks are taking place with solid security tools in place.

Only 57% are confident in their security solutions' capabilities.

Are you confident that your company's security solutions are reducing as much risk as possible?



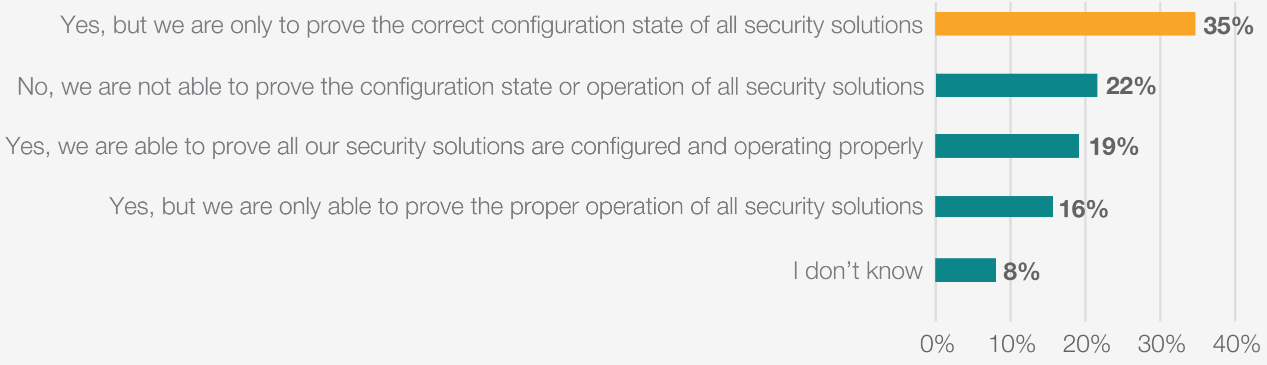
Security Assessments are Lacking

Overconfidence in a security infrastructure can be remedied by testing not only the operation and how they defend, but the configuration of the tools themselves.

Security testing is a best practice that should be followed to assess whether security tools are operating and defending as expected. When asked if they have proof that verifies that every security solution is configured correctly, and operating and defending properly, only 35 percent answered yes.

Only 35% Verify Their Security Solutions Are Defending Correctly.

Does your company have proof which verifies that every security solution is configured correctly, and operating (defending) properly?



The survey indicated that more than 50 percent of respondents were reactive to a security breach or attack, rather than proactive. While 70 percent indicated they had regularly scheduled testing, for 65 percent of respondents, that testing is taking place at intervals greater than once per month.

Security testing at intervals greater than once per month leaves an organization vulnerable. Malware attacks evolve constantly and DDOS attacks change. If tested once a month, there could potentially be tens, if not hundreds or thousands, of vulnerabilities that could be missed by security solutions. According to CVE Details, a vulnerability analysis tool from Mitre Corporation, there were a total of 16,556 vulnerabilities published in 2018, with 1,639 greater than an 8 in severity. In 2019, there were a total of 12,174 vulnerabilities published, with 1,118 greater than 8 in severity through December 13, 2019.

Finally, it is a best practice to ensure that a team is fully prepared in the inevitable event of a cyberattack. However, less than 50 percent of those surveyed said that they regularly practice how to remediate and recover from a breach.

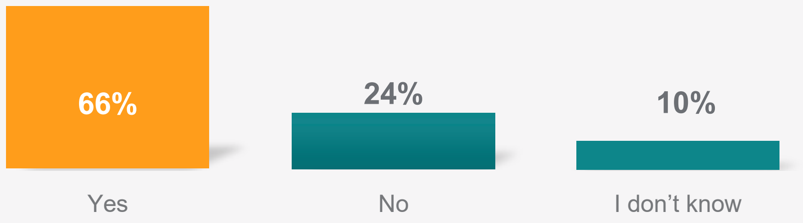
Security at a Cost

Security tool sprawl is a real issue for most organizations.

Organizations on average run 25 to 49 security tools from up to 10 different vendors, according to Enterprise Strategy Group (ESG). According to this survey, security tool sprawl does present operational impact with 66 percent reporting security solutions overlap. Looking further, 41 percent of respondents admit that the overlap is unintentional, while 57 percent say tool overlap is intentional. Reducing operational tool sprawl presents an opportunity to optimize their security solutions budget. An overwhelming 79 percent of those surveyed would remove a product if they could prove it wasn't effective. While some respondents (24 percent) would prefer redundant protection, even if proven marginally effective.

66% state their security solutions overlap functionality.

Do your company's cyber security solutions' coverage overlap with one another?

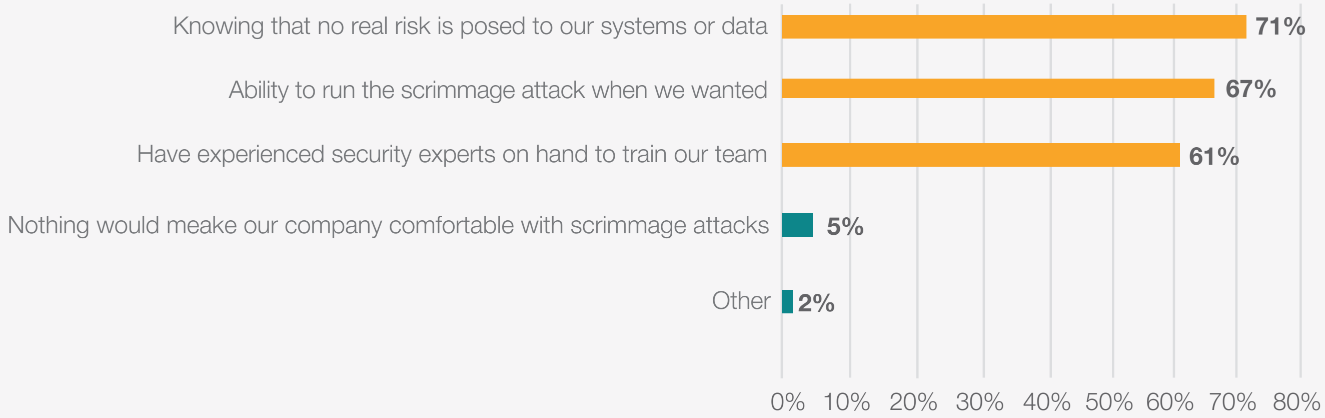


Automating Operational Security Effectiveness Testing

The survey reveals that 95 percent of security professionals are comfortable with testing automated security attacks in production. Further, 86 percent of those surveyed would find value in a solution that can find current vulnerabilities in a company's security posture and provide recommendations to remediate.

95% Are Comfortable with Automated Security Scrimmage Attacks.

In your opinion, what would make your company more comfortable with automated scrimmage security attacks?



Conclusion

Security professionals are faced with a flood of cyberattacks. They are aware of the threats and vulnerabilities to their organizations, but they cope with this by throwing security solutions or tools at the problem with overconfidence that these tools perform as expected. Ongoing security testing of their solutions' configurations and operation would provide security professionals with confidence and proof that their security solutions effectively protect their organizations while providing opportunities to save resources.

Methodology

Keysight commissioned Dimensional Research to conduct this survey in the field in November 2019. A total of 307 participants that strategize, architect, manage and operate enterprise security solutions completed the survey. Participants were from all five continents. They represented large (48%), medium (41%), and small (11%) organizations across a wide variety of industries. Researchers administered the survey electronically, and participants were offered a token compensation for their participation.

About Keysight Technologies

Keysight Technologies, Inc. (NYSE: KEYS) is a leading technology company that helps enterprises, service providers and governments accelerate innovation to connect and secure the world. Keysight's solutions optimize networks and bring electronic products to market faster and at a lower cost with offerings from design simulation, to prototype validation, to manufacturing test, to optimization in networks and cloud environments. Customers span the worldwide communications ecosystem, aerospace and defense, automotive, energy, semiconductor and general electronics end markets. Keysight generated revenues of $4.3B in fiscal year 2019. More information is available at www.keysight.com.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus